Third Way

US Global Cybercrime Cooperation: A Brief Explainer
Author(s): Allison Peters and Anisha Hindocha
Third Way (2020)
Stable URL: https://www.jstor.org/stable/resrep25041
Accessed: 18-01-2024 20:45 +00:00

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.

Your use of the JSTOR archive indicates your acceptance of the Terms & Conditions of Use, available at https://about.jstor.org/terms

Third Way is collaborating with JSTOR to digitize, preserve and extend access to this content.

This content downloaded from 193.19.205.136 on Thu, 18 Jan 2024 20:45:10 +00:00
All use subject to https://about.jstor.org/terms

THIRD WAY

MEMO *Published June 26, 2020 • 19 minute read*

US Global Cybercrime Cooperation: A Brief Explainer

Allison Peters
Deputy Director of the National Security Program
@ThirdWayNatSec

Anisha Hindocha
National Security Fellow, 2019-2020
@ThirdWayNatSec

Takeaways

Cybercrime is a persistent and transnational threat with the rates in the United States estimated to have up to quadrupled during the COVID-19 pandemic. Unfortunately, law enforcement in the United States and globally has struggled to keep up with this crime, resulting in a considerable enforcement gap that allows cybercriminals to operate with near impunity. In the United States, only 3 in 1,000 malicious cyber incidents will ever see an arrest and the global enforcement gap is likely to be similar. [1]

The investigation of one cybercrime case often involves criminal justice systems in many different countries, requiring intense international cooperation to bring the

This content downloaded from 193.19.205.136 on Thu, 18 Jan 2024 20:45:10 +00:00
All use subject to https://about.jstor.org/terms

perpetrators to justice. The United States is a member of a number of formal and informal mechanisms that help facilitate this cooperation. This includes being a party to a number of binding treaties—particularly the only global cybercrime treaty known as the Budapest Convention—as well as a member of key networks and in multilateral forums. The United States is also a member of a number of entities aimed at developing norms to guide the behavior of nation-states in cyberspace where cooperation in cybercrime investigations is encouraged.

This memo includes an explainer of the threat and these cooperation mechanisms in three sections:

- A brief overview of the cybercrime threat and the need for strengthened global cooperation to combat it;
- A mapping of the existing infrastructure on global cybercrime cooperation that the United States is a participant in, including international organizations and treaties, and efforts to undermine this infrastructure; and
- A brief discussion of the existing forums for cyberspace norm development that the United States is a member of and the intersection with cybercrime enforcement.

As the Trump Administration continues to disengage and pull funding from international organizations, some countries, particularly China and Russia, are working to fill this void and promote their vision of Internet control in different cyber-related forums. It is critically important that Congress understands the international infrastructure for global cybercrime cooperation, promotes US leadership within these entities, and ensures they have adequate funding to pursue their efforts. [2]

Global cooperation is required to counter the growing and often transnational threat of cybercrime.

Cybercrime is a threat that continues to grow in size and scope, hitting governments, businesses, organizations, and individuals in the United States and around the globe. Criminals can now easily create whole new categories of crime that can easily cross borders with the tap of a keyboard. Investigating these crimes and imposing consequences on the perpetrators often requires strong cooperation between criminal justice actors in the United States and those in other countries.

This content downloaded from 193.19.205.136 on Thu, 18 Jan 2024 20:45:10 +00:00
All use subject to https://about.jstor.org/terms

While global statistics on cybercrime are difficult to ascertain, the data that is available tells us that cybercrime appears to be increasingly pervasive with the costs of attacks growing exponentially. [3] Some estimates put the global cost of cybercrime in excess of $6 trillion annually by 2021, up from $3 trillion in 2015. [4] A 2013 United Nations (UN) draft survey found that a majority of the 69 countries polled said cybercrime was increasing or strongly increasing. [5]

Cybercrime is conducted by a range of actors, including state and non-state actors with a variety of different motivations. Some US assessments indicate organized criminals and lone cybercriminals are generally motivated by financial reasons, while nation-state actors tend to be more focused on destroying or compromising victim data. [6]

Unfortunately, criminal justice actors in the United States and globally have struggled to keep pace with the rising rate of cybercrime perpetrated by such a wide range of different actors with a variety of motives. In the United States alone, only 3 in 1,000 cyber incidents reported to the Federal Bureau of Investigations (FBI) see an arrest. [7] And some available global data indicates that the enforcement gap is no better in many other countries. [8]

Part of the reason this enforcement gap is so large is because many cybercriminals are not located in the United States and the investigation of these crimes, therefore, requires the cooperation of government actors in other countries who may be unable or unwilling to help in bringing these actors to justice. [9] A single cybercrime incident can hit countless victims in multiple countries independent of the location of the perpetrators, which means cybercrime investigations must frequently involve criminal justice systems in many different locations. For example, one cybercrime ring alone targeted over 100 financial institutions in more than 40 countries with its malware and the arrest of its leader required the cooperation of the FBI with five different countries' police, private cybersecurity companies, and the European Union's police cooperation agency known as EUROPOL. [10]

Reducing the rate of cybercrime in the United States and lowering the enforcement gap can only be achieved if the United States has the mechanisms and political leadership in place to improve global cooperation in these cases and means for eliciting cooperation if needed. Fortunately, the United States is a member of a number of bodies and mechanisms to help facilitate this cooperation.

The United States is a member of numerous bodies and mechanisms that facilitate global cooperation on cybercrime.

There are numerous existing organizations, networks, agreements, and treaties that the United States is a participant in or member of that play a role in facilitating cross-border

This content downloaded from 193.19.205.136 on Thu, 18 Jan 2024 20:45:10 +00:00
All use subject to https://about.jstor.org/terms

cooperation in cybercrime cases. This includes one-on-one agreements the United States has in place with other countries (or bilateral agreements) and those that are regional or global in nature (or multilateral agreements). The below maps some of the components of this infrastructure on global cybercrime cooperation. This infrastructure could be undermined by recent efforts supported by countries that endorse an authoritarian model of Internet control.

I. Multilateral Treaties

Convention on Cybercrime of the Council of Europe (Budapest Convention)

The Budapest Convention, opened for signatures in 2001, is the only legally binding international treaty on cybercrime. It sets common standards on investigations and facilitates criminal justice cooperation in cybercrime cases for its 65 member countries. [11] The treaty has been ratified by many non-Council of Europe members, including by the United States (which

This content downloaded from 193.19.205.136 on Thu, 18 Jan 2024 20:45:10 +00:00
All use subject to https://about.jstor.org/terms

holds observer status in the Council) in 2006. [12] The treaty is important because it provides a guidepost for nations to create and harmonize their own comprehensive national legislation on cybercrime. If done adequately, this helps ensure the legal framework is in place to allow for US cooperation with these countries in cybercrime cases. The Budapest Convention has also served as the basis of other binding regional cooperation agreements on cybercrime that the United States has been supportive of. [13] It is not a static treaty and can be updated to meet evolving needs, as is currently being done for a new protocol dealing with electronic evidence. [14] Civil society groups have called for ensuring that human rights safeguards are strongly protected in these updates. [15]

UN Convention against Transnational Organized Crime (UNTOC)

The UN Convention against Transnational Organized Crime came into force in 2003 and is another legally binding mechanism that the United States is a party to ever since its ratification in 2005. [16] While this Convention is aimed at preventing and combatting transnational organized crime, the US government has noted that its provisions are sometimes used to facilitate cooperation in cybercrime cases. This may be particularly helpful since 190 countries are party to this Convention, so it has wide reach. [17]

Inter-American Convention on Mutual Legal Assistance of the Organization of American States (OAS)

Similarly, while this Convention is not specific to cybercrime, its provisions allow for the United States to request from and provide legal assistance to OAS members, which could help facilitate regional cooperation in cybercrime cases. [18]

Treaties and Agreements to Facilitate US Cybercrime Cooperation

Multilateral

Budapest Convention: The only legally binding global treaty on cybercrime.

UN Convention against Transnational Organized Crime (UNTOC): A legally binding global treaty to prevent and combat transnational organized crime that can facilitate cooperation in some cybercrime cases.

Inter-American Convention on Mutual Legal Assistance of the Organization of American States (OAS): A regional treaty that can facilitate cooperation among OAS member states in criminal cases.

Bilateral

This content downloaded from 193.19.205.136 on Thu, 18 Jan 2024 20:45:10 +00:00
All use subject to https://about.jstor.org/terms

Mutual Legal Assistance Treaties (MLATs) and Mutual Legal Assistance Agreements (MLAAs): Treaties and agreements that formally establish procedures for the US to request from and provide legal assistance to other countries, including in cybercrime cases.

CLOUD Act Agreements: Agreements that could be signed between the US and other governments that meet privacy and civil liberties standards regarding the sharing of data across borders.

Extradition treaties: Allows the US to request the surrender of cybercriminals from another country for prosecution or punishment for crimes committed in America.

II. Bilateral Treaties and Agreements

The United States has signed numerous treaties and agreements directly with other countries that are critical in facilitating US cooperation with those governments in cybercrime investigations and prosecutions, including by allowing for the collection and sharing of evidence across borders. This includes:

Mutual Legal Assistance Treaties (MLATs) and Mutual Legal Assistance Agreements (MLAAs)

MLATs and MLAAs are agreed upon directly between the United States and other countries and they obligate the two sides to produce documents and other evidence, summon witnesses, issue warrants, and comply with agreed upon processes to do so if assistance requests in criminal cases are received. They are the most common way the United States requests assistance from other countries in criminal matters, including in cybercrime cases. As of 2018, the United States had entered into MLATs with 65 other nations and the EU. [19] The United States also has an MLAA with China, as well as one with the American Institute in Taiwan and the Taipei Economic and Cultural Representative Office. [20]

CLOUD Act Agreements

The United States is one of a small number of countries where the most data is collected and stored, which means each year the US Department of Justice fields an enormous number of requests from foreign governments who seek access to electronic evidence stored in this country for cybercrime and other criminal cases. This has caused a large backlog of requests and significant delays in response time, which hinders the timely investigation of cybercrime cases. [21] In 2018, Congress passed the "Clarifying Lawful Overseas Use of Data Act" (CLOUD Act, P.L. 115-141) to allow the United States to enter into negotiations for executive

This content downloaded from 193.19.205.136 on Thu, 18 Jan 2024 20:45:10 +00:00
All use subject to https://about.jstor.org/terms

agreements with other nations who can meet certain privacy and civil liberties standards in order to facilitate cross-border data sharing directly between US companies and foreign governments (hopefully reducing the backlog and delays). [22] The United States has entered into such an agreement with the United Kingdom and is negotiating another with Australia. [23]

Extradition Treaties

The United States has signed extradition treaties with over 100 countries, which establish a process whereby one country surrenders an individual to another country for prosecution or punishment for crimes committed in the requesting country's jurisdiction. [24] These treaties are critical because they allow the United States to request the extradition of accused cybercriminals to be brought to this country to stand trial. But the United States does not have such a treaty with some of the countries that are most problematic in terms of cybercrime emanating from their borders such as Iran and North Korea. [25] More recent treaties have also included a "dual criminality" requirement, which requires the charged conduct to be criminalized in both the requesting and requested jurisdictions for an extradition to proceed. This can create challenges for the United States in facilitating cooperation with countries where their national laws have not been updated to criminalize different forms of cybercrime. [26]

The United States' membership in INTERPOL, the world's largest police organization, can also help facilitate extradition, and other forms of cooperation, in cybercrime cases. [27] INTERPOL allows for the United States to send and respond to requests for information and assistance in criminal investigations. [28] Its red notice system is the closest thing that exists to an international arrest warrant and, through this system, the United States can circulate notices for cybercriminals that are wanted for extradition to other countries so they can try to locate and arrest the individual(s). [29]

Other Bilateral Cooperation Initiatives

The United States is engaged in numerous bilateral cybercrime cooperation initiatives with other nations. These dialogues are aimed at, among other things, building on existing treaties like the Budapest Convention to increase cooperation in cybercrime investigations. [30] The United States also contributes to bilateral and regional capacity building efforts on cybercrime, which can help boost the capability of countries to be able to cooperate in these investigations. [31]

This content downloaded from 193.19.205.136 on Thu, 18 Jan 2024 20:45:10 +00:00
All use subject to https://about.jstor.org/terms

III. International Organizations, Forums, and Networks

In addition to these formal agreements, there are many international organizations, forums, and networks the United States is a member of or participant in that help facilitate informal cooperation. These mechanisms can be important to facilitate the exchange of information in criminal cases and sharing of expertise and experience, particularly between the United States and countries where no formal treaties exist or diplomatic relationships are not strong. These include:

United Nations Commission on Crime Prevention and Criminal Justice (CCPCJ)

The UN CCPCJ was established in 1992 and is the principal UN policymaking body on all issues related to crime prevention and criminal justice, including cybercrime. The United States is currently an elected member of the Commission, providing the US government with a forum to discuss and exchange expertise and experience on cybercrime issues. [32] The CCPCJ also governs the work of the UN Office on Drugs and Crime (UNODC), which educates countries on cybercrime and conducts important capacity building programming to help boost the capability of other countries to investigate it. [33] It is also the preparatory body for what is colloquially known as the UN Crime Congress—a high-level meeting of government officials held every five years to discuss important criminal matters where cybercrime has been a primary focus in recent years. [34]

This content downloaded from 193.19.205.136 on Thu, 18 Jan 2024 20:45:10 +00:00
All use subject to https://about.jstor.org/terms

Organization for Security and Co-operation in Europe (OSCE)

The United States is a participating State in the OSCE, which is the world's largest regional security organization and includes 57 countries from North America, Europe, and Asia. [35] The organization has worked to develop confidence-building measures (CBMs) to reduce conflict between countries that arises from the increased use of information and communications technologies (ICTs). These CBMs encourage countries to put in place national legislation to facilitate the voluntary cooperation between law enforcement agencies to counter the criminal use of ICTs and have a point of contact to facilitate communication. [36] The OSCE has also implemented projects to build the capacity of countries in regions such as Eastern Europe on cybercrime. [37]

Organization of American States (OAS) Inter-American Cooperation Portal on Cyber-Crime and Working Group

The United States participates in the Inter-American Cooperation Portal on Cyber-Crime, which was created to facilitate information exchange from government experts with cybercrime responsibilities within OAS member states and streamline cybercrime investigations and extraditions. [38] The OAS' Cyber-Crime Working Group seeks to develop mechanisms to enhance and strengthen cooperation among its regional members in the area of cybercrime. [39]

Group of Seven (G7)'s 24/7 Cybercrime Network

The G7 is a forum to bring together the leaders of the world's leading industrial nations, including the United States. Its 24/7 Network, which includes more than 70 nations, establishes points of contact to respond to urgent requests from governments to preserve digital evidence, including in cybercrime cases. [40]

The United States also participates in the Council of Europe's Network of 24/7 Contact Points and INTERPOL's secure communication network known as I-24/7, which is a tool that allows for intelligence and information sharing during cybercrime investigations. [41]

European Union Agency for Law Enforcement Cooperation (EUROPOL)'s Joint Cybercrime Action Taskforce (J-CAT)

As one of 16 member countries in EUROPOL's J-CAT, the United States has sent liaisons from the FBI and Secret Service to participate in the Taskforce's standing team of cyber liaisons and work with other members to support joint intelligence-led, coordinated action against specific cybercrime threats. It has had a number of successes in arresting cybercriminals. [42]

Global Forum on Cyber Expertise (GFCE)

This content downloaded from 193.19.205.136 on Thu, 18 Jan 2024 20:45:10 +00:00
All use subject to https://about.jstor.org/terms

The United States is a member of the GFCE and participates in meetings of its Cybercrime Working Group. The GFCE is comprised of public and private sector members and works to strengthen international cooperation on cyber capacity building, including by sharing research and expertise on cybercrime and serving as a clearing house for projects. [43]

While these agreements, organizations, and networks might help to facilitate the United States' cooperation with other governments on cybercrime enforcement, efforts underway by governments with competing visions on cybercrime cooperation might hurt progress in this area.

In particular, Russia, with the support of China and other countries who have advocated for a more authoritarian model of state control of the Internet, has pushed for a new global cybercrime treaty at the UN. After winning a vote on a UN resolution at the end of 2019, negotiations on such a treaty will begin after an organizing meeting scheduled for August 2020. The resolution advances Russia's long-standing goal of replacing the Budapest Convention with a global treaty that more closely aligns with its vision of what international cooperation on cybercrime should look like. Broader global cooperation on cybercrime would be an important positive step, if possible, given the countries where cybercrime most often emanates from are not members of many of the above conventions and agreements. However, the vague language in the draft treaty circulated by Russia and its 2019 resolution raise a number of human rights and procedural concerns, including whether such a new global treaty would be used as a tool for targeting free speech. And a new treaty could create separate, and perhaps competing, mechanisms for global cooperation on cybercrime, leading to less not more progress. [44]

Additionally, China's efforts to work through international organizations to promote its "Digital Silk Road" and set standards on ICTs that run counter to United States' efforts, as well as rising tension between the two countries over COVID-19, could impact the effectiveness of a number of mechanisms in place for US-China cybercrime cooperation. [45]

United States efforts to push back against these moves will continue to be hindered by an American diplomatic corps that has seen growing resignations and vacancies, including the complete elimination of the State Department's top cyber diplomat under the Trump Administration, and continued attempts to slash the Department's budget, particularly the global cybercrime programming of the Bureau of International Narcotics and Law Enforcement Affairs (INL). [46] Disagreements between the Trump Administration and Congress have largely left America leaderless on cyber diplomacy despite the urgent need for strengthened global cooperation on cybercrime and other cyber-related issues.

This content downloaded from 193.19.205.136 on Thu, 18 Jan 2024 20:45:10 +00:00
All use subject to https://about.jstor.org/terms

Forums for the development of norms in cyberspace may help boost cybercrime enforcement cooperation.

The United States is a member of several bodies focused on the development of norms for nation-state behavior in cyberspace, which has been a priority area for Congress. While those forums are largely kept separate from those on cybercrime, the United States could work to better connect these debates and encourage cooperation.

The development of norms to guide responsible nation-state behavior in cyberspace has been a priority area for the US government over the last decade as governments around the globe have gained more and more cyber capabilities. Secretary of State Mike Pompeo recently stressed the importance of such norms in response to cyberattacks targeting the healthcare sector during the COVID-19 pandemic. [47] Congress has particularly stressed the importance of US leadership in such norm development. It is a component of the US International Cyberspace Policy articulated in the "Cyber Diplomacy Act of 2019" (H.R. 739) and the recently released report of the US Cyberspace Solarium Commission. [48] Members of Congress have also directly called on the State Department to step up its leadership in this area. [49]

There are a number of global forums that have been established to try to push for consensus on norms, principles, and rules governing the behavior of countries in cyberspace. Essentially more clearly defining "rules-of-the-road" specific for cyberspace. In 2015, the fourth UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (often referred to as the UN GGE), which the United States was a part of, agreed on a consensus report on the norms, principles, and rules governing state behavior in cyberspace (although a subsequent 2017 GGE failed to achieve similar consensus). The report called on nation-states to consider several voluntary measures, including creating procedures for mutual assistance in responding to cyber incidents. The United States also agreed upon the G7's 2017 Declaration on Responsible States Behavior in Cyberspace (also known as the Lucca Declaration), which committed States to consider "how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats." Now, the United States is participating in two UN processes, one is a new GGE with selected members and the other an open-ended working group open to all UN members, that are focused on further developing cyber norms. [50]

In these discussions, the United States would be wise to remind the global community of the voluntary commitments that have already been agreed upon concerning cybercrime cooperation and stress that such cooperation is inherently linked to the enforcement of norms. Discussions at the UN and in other international organizations around cybercrime are

This content downloaded from 193.19.205.136 on Thu, 18 Jan 2024 20:45:10 +00:00
All use subject to https://about.jstor.org/terms

largely kept separate from those on cyber norm development. While there may be good reasons for keeping those discussions separate, for countries that are new to this debate or lack the necessary expertise, this can be quite confusing and give the impression that the enforcement of cybercrime is completely separate from expectations of how nation-states should behave in cyberspace. [51] Yet, addressing cybercrime is inherently tied to the debates on norms—bringing cybercriminals to justice, regardless if they are state-backed, is an important component of enforcing norms. Instead of promoting fragmentation, the United States could work to better link the debates in these forums and support capacity building efforts to boost the knowledge and expertise of governments in need.

Congress must understand the international infrastructure for global cybercrime cooperation and push for US leadership and resourcing to support these efforts.

As the Trump Administration continues to disengage and pull funding from international organizations and forums that are working to boost global cooperation on cybercrime, there will be consequences. This is already resulting in a vacuum that countries who have a more authoritarian view of what Internet control means are already working to fill. And that will only undermine the established mechanisms for global cooperation on cybercrime that the United States benefits from and hurt US efforts to bring cybercriminals to justice. To ensure this doesn't happen, it is critically important that Congress understands this international infrastructure for global cybercrime cooperation, pushes back against efforts that will undermine US leadership within these entities, and ensures these mechanisms, forums, and networks have adequate funding to pursue their efforts. This means also ensuring that America has the high-level leadership to even engage in negotiations around the future direction of cybercrime cooperation to begin with.

TOPICS

CYBERSECURITY 52

ENDNOTES

This content downloaded from 193.19.205.136 on Thu, 18 Jan 2024 20:45:10 +00:00
All use subject to https://about.jstor.org/terms

1. Eoyang, Mieke, et al. "To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors." Third Way, Third Way, 29 Oct. 2018, pp. 1-2. https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors. Accessed 16 June 2020; Peters, Allison and Amy Jordan. "Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime." *Journal of National Security Law and Policy*, 13 Feb. 2020, pp. 492-493, https://jnslp.com/wp-content/uploads/2020/05/Countering-the-Cyber-Enforcement-Gap.pdf. Accessed 16 June 2020.

2. Shendruk, Amanda, et al. "Funding the United Nations: What Impact Do U.S. Contributions Have on UN Agencies and Programs?" *Council on Foreign Relations*, 8 Jun 2020, https://www.cfr.org/article/funding-united-nations-what-impact-do-us-contributions-have-un-agencies-and-programs. Accessed 16 June 2020; Congressional Research Service. "United Nations Issues: U.S. Funding to the U.N. System." 10 Mar. 2020, https://fas.org/sgp/crs/row/IF10354.pdf. Accessed 16 Jun 2020.; Gramer, Robbie and Colum Lynch. "Trump Stealthily Seeks to Choke Off Funding to U.N. Programs." Foreign Policy, 2 Oct. 2018, https://foreignpolicy.com/2018/10/02/trump-stealthily-seeks-to-choke-off-funding-to-un-programs/. Accessed 16 June 2020.

3. Bissell, Kelly and Larry Ponemon. "The Cost of Cybercrime." *Accenture Security*, 15 June 2019, pp. 17. https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf. Accessed 16 June 2020.

4. Morgan, Steve. "2019 Official Annual Cybercrime Report." *Herjavec Group*, 2019, pp. 2. https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf. Accessed 16 June 2020.

5. Permanent Mission of the United States of America. "Comments of the United States to the Draft Comprehensive Study on Cybercrime."16 Aug. 2016, https://perma.cc/9JSU-G8ZY. Accessed 16 June 2020.

6. Broadhurst, Roderic, et al. "Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime." *International Journal of Cyber Criminology*, Vol 8, Issue 1, June 2014, pp. 3 https://perma.cc/PA8W-2SMS pg 3. Accessed 16 June 2020; Deputy Attorney General Rod Rosenstein. "Report of the Attorney General's Cyber Digital Taskforce." *United States Department of Justice*, 2 July 2018, pp. 25, https://www.justice.gov/ag/page/file/1076696/download. Accessed 16 June 2020.

7. Eoyang, Mieke, et al. "To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors." *Third Way*, Third Way, 29 Oct. 2018, pp. 1-2. https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors. Accessed 16 June 2020.

8. Peters, Allison and Amy Jordan. "Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime." *Journal of National Security Law and Policy*, 13 Feb. 2020, pp. 492-493, https://jnslp.com/wp-content/uploads/2020/05/Countering-the-Cyber-Enforcement-Gap.pdf. Accessed 16 June 2020.

This content downloaded from 193.19.205.136 on Thu, 18 Jan 2024 20:45:10 +00:00
All use subject to https://about.jstor.org/terms

9. Defined by UNODC as cases "where an element or substantial effect of the offence is in another territory, or where part of the modus operandi of the offence is in another territory." Malby, Steve, et al. "Comprehensive Study on Cybercrime." United Nations Office on Drugs and Crime, Feb. 2013, pp. xxiv, https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. Accessed 16 June 2020.

10. "Mastermind Behind Eur 1 Billion Cyber Bank Robbery Arrested in Spain." Press Release, *Europol*, 26 Mar. 2018, https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain. Accessed 16 June 2020.

11. "Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY." *Council of Europe*, https://www.coe.int/en/web/cybercrime/parties-observers. Accessed 16 June 2020.

12. "Treaty List for a Specific State: United States of America." *Council of Europe*, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/country/USA?p_auth=7KdsGjzK. Accessed 16 June 2020.

13. For example: The African Union Convention on Cyber Security and Personal Data Protection; Arab Convention on Combating Information Technology Offences; Agreement on Cooperation Among the States Members of the Commonwealth of Independent States in Combating Offences Relating to Computer Information

14. "Towards a Protocol to the Budapest Convention." *Council of Europe*, 5 Sep. 2019, https://rm.coe.int/summary-towards-a-protocol-to-the-budapest-convention/1680972d07. Accessed 16 June 2020.

15. "New Protocol on cybercrime: a recipe for human rights abuse?" *European Digital Rights*, 25 July 2018, https://edri.org/new-protocol-on-cybercrime-a-recipe-for-human-rights-abuse/. Accessed 16 June 2020.

16. "12. United Nations Convention against Transnational Organized Crime." *United Nations Treaty Collection*, United Nations, 15 Nov. 2000, https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-12&chapter=18&clang=_en. Accessed 16 June 2020.

17. "United Nations Convention against Transnational Organized Crime and the Protocols Thereto." *United Nations Office on Drugs and Crime*, 29 Sep. 2003, https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html 16 June 2020; Walker, Summer. "Cyber-Insecurities? A guide to the UN cybercrime debate." *The Global Initiative Against Transnational Organized Crime*, Mar. 2019, pp. 6, https://globalinitiative.net/wp-content/uploads/2019/03/TGIATOC-Report-Cybercrime-in-the-UN-01Mar1510-Web.pdf. Accessed 16 June 2020; United Nations Office on Drugs and Crime. "Digest of organized crime cases." *United Nations Office on Drugs and Crime,* Oct. 2012, https://www.legal-tools.org/doc/ac5d7e/pdf/. Accessed 16 June 2020.

This content downloaded from 193.19.205.136 on Thu, 18 Jan 2024 20:45:10 +00:00
All use subject to https://about.jstor.org/terms

18. "Inter-American Convention on Mutual Assistance in Criminal Matters." *Department of International Law*, Organization of American States, https://www.oas.org/juridico/english/treaties/a-55.html. Accessed 16 June 2020.

19. "Mutual Legal Assistance in Criminal Matters Treaties (MLATs)" *Foreign Affairs Manuals*, Department of State, 25 Mar. 2013, https://fam.state.gov/searchapps/viewer?format=html&query=mlat&links=MLAT&url=/FAM/07FAM/07FAM0960.html#M962_1. Accessed 16 June 2020.

20. Bureau of International Narcotics and Law Enforcement Affairs. "Treaties and Agreements." *2012 International Narcotics Control Strategy Report (INCSR)*, United States Department of State, 7 Mar. 2012, https://2009-2017.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm. Accessed 16 June 2020.

21. "Performance Budget FY 2021 Congressional Submission." *Department of Justice*, Criminal Division, Feb. 2020, pp. 10. https://www.justice.gov/doj/page/file/1246356/download. Accessed 16 June 2020.

22. "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act." *White Paper*, Department of Justice, Apr. 2019, pp. 2, https://www.justice.gov/opa/press-release/file/1153446/download. Accessed 16 June 2020.

23. "Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of American on Access to Electronic Data for the Purpose of Countering Serious Crime." *Secretary of State for Foreign and Commonwealth Affairs*, Oct. 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf. Accessed 16 June 2020; "Joint Statement Announcing United States and Australian Negotiation of a CLOUD Act Agreement by U.S. Attorney General William Barr and Minister for Home Affairs Peter Dutton." *Press Release*, Department of Justice, 7 Oct. 2019, https://www.justice.gov/opa/pr/joint-statement-announcing-united-states-and-australian-negotiation-cloud-act-agreement-us. Accessed 16 June 2020.

24. Garcia, Michael John and Charles Doyle. "Extradition To and From the United States: Overview of the Law and Contemporary Treaties." *Congressional Research Service*, 4 Oct. 2016, https://crsreports.congress.gov/product/pdf/RL/98-958.Accessed 16 June 2020.

25. "Title 18 – Crimes and Criminal Procedure." *Department of State*, https://2009-2017.state.gov/documents/organization/71600.pdf. Accessed 16 June 2020.

26. Peters, Allison and Amy Jordan. "Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime." *Journal of National Security Law and Policy*, 13 Feb. 2020, pp. 499, https://jnslp.com/wp-content/uploads/2020/05/Countering-the-Cyber-Enforcement-Gap.pdf. Accessed 16 June 2020.

This content downloaded from 193.19.205.136 on Thu, 18 Jan 2024 20:45:10 +00:00
All use subject to https://about.jstor.org/terms

27. "Member Countries." *Interpol*, https://www.interpol.int/en/Who-we-are/Member-countries. Accessed 16 June 2020.

28. Office of the Inspector General. "The United States National Central Bureau of Interpol Audit Report." *Department of Justice*, Sep. 2009, https://oig.justice.gov/reports/plus/a0935/final.pdf. Accessed 16 June 2020.

29. Department of Justice. "611. Interpol Red Notices." *Department of Justice*, Archives, 22 Jan. 2020, https://www.justice.gov/archives/jm/criminal-resource-manual-611-interpol-red-notices. Accessed 16 June 2020.

30. "Joint Statement on the Inaugural U.S.-Dutch Cyber Dialogue." Media Note, *United States Department of State, Office of the Spokesperson*, 20 May 2019, https://www.state.gov/jointstatement-on-the-inaugural-u-s-dutch-cyber-dialogue/. Accessed 12 June 2020; "Joint Statement on the Third U.S.-Estonia Cyber Dialogue." Media Note, *United States Department of State, Office of the Spokesperson*, 7 June 2019, https://www.state.gov/joint-statement-on-the-third-us-estonia-cyber-dialogue/. Accessed 12 June 2020.

31. Office of the Coordinator for Cyber Issues. "Cybercrime." *Department of State*, Aug. 2015, https://2009-2017.state.gov/documents/organization/255007.pdf. Accessed 16 June 2020.

32. "Members of the Commission on Crime Prevention and Criminal Justice." *United Nations Office on Drugs and Crime*, United Nations, 1 Jan. 2019, https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_membership_1_Jan_2019_20181205_rev2.pdf. Accessed 16 June 2020.

33. "Commission on Crime Prevention and Criminal Justice." United Nations Office on Drugs and Crime, https://www.unodc.org/unodc/en/commissions/CCPCJ/index.html. Accessed 16 June 2020.

34. "Crime Congress 2015: A focus on Cybercrime." *United Nations Office on Drugs and Crime*, 5 Mar. 2015, https://www.unodc.org/unodc/en/frontpage/2015/March/focus_its-a-crime_-cybercrime.html. Accessed 16 June 2020.

35. "Who We Are." *Organization for Security and Co-operation in Europe*, https://www.osce.org/who-we-are. Accessed 16 June 2020.

36. "OSCE Confidence-Building Measures for Cyberspace." *The NATO Cooperative Cyber Defence Centre of Excellence*, https://ccdcoe.org/incyder-articles/osce-confidence-building-measures-for-cyberspace/. Accessed 16 June 2020.

37. OSCE Secretariat and Chairmanship. "Criminal justice practitioners explore how to effectively counter cybercrime and cyber-enabled crime at OSCE conference in Vienna." *Organization for Security and Co-operation in Europe*, 27 May 2019, https://www.osce.org/secretariat/420965. Accessed 16 June 2020.

This content downloaded from 193.19.205.136 on Thu, 18 Jan 2024 20:45:10 +00:00
All use subject to https://about.jstor.org/terms

38. "Inter-American Cooperation Portal on Cyber-Crime." *Organization of American States*, Department of Legal Cooperation, https://www.oas.org/juridico/english/cyber.htm. Accessed 16 June 2020.

39. "Frequently Asked Questions." *Organization of American States*, Department of Legal Cooperation, http://www.oas.org/juridico/english/cyber_faq_en.htm#2. Accessed 16 June 2020.

40. Ott, Chris. "What You Should Know About the 24/7 Cybercrime Network." *Davis Wright Tremaine*, 28 June 2018, https://www.dwt.com/files/uploads/documents/publications/What%20You%20Should%20Know%20About%20The%2024.pdf. Accessed 16 June 2020.

41. "Convention on Cybercrime." *Council of Europe*, 23 Nov. 2001, pp. 20-21, https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest__/7_conv_budapest_en.pdf. Accessed 16 June 2020; "Databases." *Interpol*, https://www.interpol.int/en/How-we-work/Databases. Accessed 16 June 2020.

42. "Joint Cybercrime Action Taskforce (J-CAT)." *Europol*, https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce. Accessed 16 June 2020.

43. "About the GFCE." Global Forum on Cyber Expertise, https://thegfce.org/about-the-gfce/. Accessed 16 June 2020.

44. Hakmeh, Joyce and Allison Peters. "A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet." *Council on Foreign Relations*, 13 Jan. 2020, https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet. Accessed 16 June 2020.

45. Lee, Kristine and Alexander Sullivan. "People's Republic of the United Nations." *Center for a New American Security*, May 2019, pp. 16-17,https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Report-China-IO-final-web-b.pdf?mtime=20190513092354. Accessed 16 June 2020; Levite, Ariel (Eli) and Lyu Jinghua. "Chinese-American Relations in Cyberspace: Toward Collaboration or Confrontation?" *Carnegie Endowment for International Peace*, 24 Jan. 2019, https://carnegieendowment.org/2019/01/24/chinese-american-relations-in-cyberspace-toward-collaboration-or-confrontation-pub-78213. Accessed 16 June 2020.

This content downloaded from 193.19.205.136 on Thu, 18 Jan 2024 20:45:10 +00:00
All use subject to https://about.jstor.org/terms

46. Blair, Jason. "Department of State Integrated Action Plan Could Enhance Efforts to Reduce Persistent Overseas Foreign Service Vacancies." *Government Accountability Office*, Mar. 2019, https://www.gao.gov/assets/700/697281.pdf. Accessed 16 June 2020; Gramer, Robbie and Elias Groll. "Can State's New Cyber Bureau Hack It?" Foreign Policy, 18 Jan. 2019, https://foreignpolicy.com/2019/01/18/state-department-cyber-security-cyber-threats-russia-china-diplomacy-capitol-hill-lawmakers-pompeo/. Accessed 16 June 2020; Hindocha, Anisha. "2020 Reader's Guide to Understanding the US Cyber Enforcement Architecture and Budget." *Third Way*, Third Way, 26 Mar. 2020, https://www.thirdway.org/report/2020-readers-guide-to-understanding-the-us-cyber-enforcement-architecture-and-budget. Accessed 16 June 2020.

47. "The United States Concerned by Threat of Cyber Attack Against the Czech Republic's Healthcare Sector." Press Statement, *Department of State, Michael R. Pompeo*, 17 Apr. 2020, https://www.state.gov/the-united-states-concerned-by-threat-of-cyber-attack-against-the-czech-republics-healthcare-sector/. Accessed 16 June 2020.

48. United States, Congress, House, Cyber Diplomacy Act of 2019, *Congress.gov*, https://www.congress.gov/bill/116th-congress/house-bill/739/text. 116th Congress, 1st session, House Resolution 739, introduced 24 Jan 2019; "Report." *Cyberspace Solarium Commission*, Mar. 2020, pp. 46-50, https://www.solarium.gov/report. Accessed 16 June 2020.

49. "Himes Calls on State Department to Advance International Cyber Norms." Press Release, *Office of Congressman Jim Himes*, 6 Feb. 2020, https://himes.house.gov/media-center/press-releases/himes-calls-state-department-advance-international-cyber-norms. Accessed 16 June 2020.

50. "UN GGE and OEWG." Geneva Internet Platform, Digital Watch Observatory, https://dig.watch/processes/un-gge. Accessed 16 June 2020.

51. Hakmeh, Joyce and Allison Peters. "A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet." *Council on Foreign Relations*, 13 Jan. 2020, https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet. Accessed 16 June 2020.

This content downloaded from 193.19.205.136 on Thu, 18 Jan 2024 20:45:10 +00:00
All use subject to https://about.jstor.org/terms